THE COMPLEXITY OF CHECKING IDENTITIES OVER FINITE GROUPS

GÁBOR HORVÁTH AND CSABA SZABÓ

Abstract. We analyze the computational complexity of solving a single equation and checking identities over finite meta-abelian groups. Among others we answer a question of Goldmann and Russel from '98: We prove that it is decidable in polynomial time whether or not an equation over the six element group S_3 has a solution.

1. Introduction

The computational complexity of the word problem in algebra is of greater and greater interest. In this paper we present results about the computational complexity of checking identities over finite groups. We use standard notations in computational complexity (see [3]).

In 1997 Ross Willard gave a talk at The Fields Institute where he presented several results and problems concerning algebraic complexity questions about rings. He defined two versions of the word problem. There are two kinds of words. A *term* on an algebra $\mathbf{A}$ is an expression that can be obtained using (iterated) compositions of the basic operations and projections. *Projections* are trivial operations satisfying $p_i^n(x_1, \ldots, x_n) = x_i$. A *polynomial* on an algebra $\mathbf{A}$ is an expression that can be obtained using (iterated) compositions of the basic operations, projections and nullary, constant operations. The two versions of the word problem are the term equivalence (TERM-EQ), and the polynomial equivalence (POL-EQ) problems.

Definition 1. Let $\mathbf{A}$ be an algebra. Two terms (polynomials) t_1 and t_2 are called *equivalent* ($t_1(x_1, \ldots, x_n) \equiv t_2(x_1, \ldots, x_n)$ or shortly $t_1 \equiv t_2$) if the values of the two terms (polynomials) are equal at every substitution from $\mathbf{A}$. An instance of the term (polynomial) equivalence problem (TERM-EQ $\mathbf{A}$, POL-EQ $\mathbf{A}$ is a pair of terms (polynomials) t_1 and t_2 with the question whether or not the two terms (polynomials) are equivalent.

For finite structures there is an obvious algorithm to decide these problems. Indeed, one can check every possible substitution, and if the

two terms (polynomials) agree at all of them then they are equivalent. On the other hand, if one finds a tuple of elements NOT satisfying the equation, then it can be showed in polynomial time that the two words are not equivalent. Hence for finite algebras both equivalence problems are obviously in coNP. In what follows, all algebras will be finite.

Thus two terms, t_1 and t_2 are equivalent if and only if $t_1 = t_2$ is an identity over $\mathbf{A}$. In case $\mathbf{A}$ is a group, this is equivalent to $t_1 t_2^{-1} \equiv 1$. Hence, we introduce the following definition, often used in group theory.

Definition 2. A term over a group is called an identity if it is equivalent to 1, the identity element of the group.

Willard in his talk discussed these two problems for rings. It was already known ([5]) that for a commutative ring $\mathbf{R}$ the TERM-EQ problem is in P if $\mathbf{R}$ is nilpotent and coNP-complete otherwise. Burris and Lawrence proved in [2] that the same holds for rings in general. Following their proof it is easy to see that for a nilpotent ring $\mathbf{R}$ the problem POL-EQ $\mathbf{R}$ is in P and it is a straightforward consequence of their result that if the ring is not nilpotent, then POL-EQ $\mathbf{R}$ is coNP-complete.

For groups the answer is far less complete. An unpublished result of Burris and Lawrence (1994) is the following.

Theorem 3. *Let* $\mathbf{G}$ *be a group. If* $\mathbf{G}$ *is nilpotent, then* TERM-EQ $\mathbf{G}$ *is in P. If* $\mathbf{G}$ *is not solvable, then* TERM-EQ $\mathbf{G}$ *is coNP-complete.*

In this paper we would like to extend these results for a class of solvable non-nilpotent groups. We prove that several kinds of semidirect products admit polynomial time solvable TERM-EQ problem. For example we prove that checking identities is easy for the dihedral groups, for the alternating group A_4, for the wreath product of two cyclic groups, etc.

The other problem to investigate is the complexity of solving equations and systems of equations over finite algebras. These problems arise from unification theory ([6]), formal languages ([11]) and, naturally, from universal algebra.

Definition 4. Let $\mathbf{A}$ be an algebra. The input of the polynomial satisfiability problem (POL-SAT $\mathbf{A}$) is a pair of polynomials s and t with the question whether there is a substitution of the variables from $\mathbf{A}$ such that the values of the two polynomials are the same.

Definition 5. Let $\mathbf{A}$ be an algebra. The input of the polynomial system-satisfiability problem (POL-SYS $\mathbf{A}$) are $2n$ polynomials $s_1, \ldots, s_n$ and $t_1, \ldots, t_n$ with the question whether there is a substitution of the variables from $\mathbf{A}$ such that $s_i = t_i$ for all $i = 1, \ldots, n$.

The complexity POL-SYS is fully characterized for groups in [4] and [8]:

Theorem 6. *Let* $\mathbf{A}$ *be a group. The problem* POL-SYS $\mathbf{A}$ *is in P if* $\mathbf{A}$ *is Abelian and it is NP-complete otherwise.*

The characterization of solving a single equation looks more complicated, though ([4]).

Theorem 7. *Let* $\mathbf{G}$ *be a group. If* $\mathbf{G}$ *is nilpotent, then* POL-SAT $\mathbf{G}$ *is in P. If* $\mathbf{G}$ *is not solvable, then* POL-SAT $\mathbf{G}$ *is coNP-complete.*

The result tells nothing about non-nilpotent solvable groups. Goldmann and Russel explicitly ask in [4] to decide the complexity of solving an equation over S_3.

The POL-SAT problem was first examined for monoids and semigroups. Klíma [7] has analyzed the question for semigroups of size at most 6. He proved for almost all of these semigroups that solving an equation is in either in P or NP-complete. The only remaining case is the 6 element "monoid" S_3. He conjectures that the problem is in P.

In this paper we show the following: If $\mathbf{G} \simeq \mathbf{A} \rtimes \mathbf{B}$, where $\mathbf{A} \simeq \mathbf{Z_p}$ and $\mathbf{B} \simeq \mathbf{Z_q}$ for some primes p and q, then POL-SAT $\mathbf{G}$ is in P. Thus, with $\mathbf{Z_3} \simeq \mathbf{A}$ and $\mathbf{Z_2} \simeq \mathbf{B}$ we answer the questions of both Goldmann and Russel and Klíma.

The result suggests that the complexity of TERM-EQ and POL-SAT for a finite algebra $\mathbf{A}$ is always the same. This is far from to be true. Seif and Szabó present a 10 element semigroup (see [10]) for which the term-equivalence problem is decidable in polynomial time and the POL-SAT problem is coNP-complete. An even stronger result of Klíma is the following (see [7]):

Theorem 8. *There is a semigroup* $\mathbf{S}$ *of size 24 such that* POL-SAT $\mathbf{S}$ *is NP-complete and* POL-EQ $\mathbf{S}$ *is in P.*

It may happen, though, that the complexity of the two problems coincide in case of groups. At this point we do not even know the answer for $\mathbf{S}_4$.

2. Semidirect products

In this section we will prove for a class of non-nilpotent groups that the POL-EQ problem (so the TERM-EQ problem also) can be solved in polynomial time. The group operation will always be multiplication. The identity element of a group will be denoted by 1. The following method will play a crucial role in our investigation.

Collecting procedure: Let $\mathbf{G} \simeq \mathbf{A} \rtimes \mathbf{B}$ where $\mathbf{A}$ is Abelian and let $t = x_1 x_2 \dots x_k$ be a group polynomial over $\mathbf{G}$. Without loss of generality we assume that the x_i are constants or variables over $\mathbf{G}$. Every element of $\mathbf{G}$ can be uniquely written of the form ba where $a \in \mathbf{A}$ and $b \in \mathbf{B}$. So we write x_i of the form $b_i a_i$ where $a_i \in \mathbf{A}$ and $b_i \in \mathbf{B}$. Collecting the elements of $\mathbf{B}$ to the left we obtain

$$t = (b_1 b_2 \dots b_k) \cdot \left(a_1^{b_2 b_3 \dots b_k} a_2^{b_3 \dots b_k} \dots a_{k-1}^{b_k} a_k \right).$$

This term is an identity if and only if both

$$b_1 b_2 \dots b_k \tag{1}$$

and

$$\left(a_1^{b_2 b_3 \dots b_k} a_2^{b_3 \dots b_k} \dots a_{k-1}^{b_k} a_k \right) \tag{2}$$

are identities (i.e. both are identically 1 for all substitutions over $\mathbf{G}$). Let us examine the latter expression. Substitute $a_i = 1$ for all i, where x_i was a variable, not constant. Then we get $t' = c_1^{w_1} c_2^{w_2} \dots c_m^{w_m}$, where all c_is are constants from $\mathbf{A}$ and w_i is a word over $\mathbf{B}$ (let us call t' the *constant part* of (2)). Let us fix j. Substituting $a_i = 1$ for $i \neq j$ (where a_i is not constant) we obtain an identity of the form $t'_j t'$ where $t'_j = a_j^{h_1} a_j^{h_2} \dots a_j^{h_l}$ and l is the number of the occurrences of x_j in t and h_i is a semigroup polynomial over $\mathbf{B}$ for every $1 \leq i \leq l$. Obviously, (2) is an identity if and only if t' and t'_j are identities for every $1 \leq j \leq k$. Hence we are looking for the complexity of checking whether or not $b_1 b_2 \dots b_k$, t and t'_j are all identities.

Lemma 9. *Let $\mathbf{F}$ be a field of prime characteristic p and $\mathbf{H} \leq \mathbf{F}^*$. For a polynomial $f(\bar{x}) \in \mathbf{F}[x_1, x_2, \dots, x_k]$ it can be checked in polynomial time whether or not it vanishes on $\mathbf{H}$.*

Proof. Let a be a generator of $\mathbf{F}^*$ and let $\mathbf{H} = \langle a^t \rangle$. Putting $z_j = x_j^t$ we have $f(\bar{x})$ is identically 0 over $\mathbf{H}$ if and only if $f(\bar{z})$ is identically 0 over $\mathbf{F}^*$. A polynomial $g \in \mathbf{F}[x_1, \dots, x_k]$ admits this latter property if and only if $g = \sum (x_i^{q-1} - 1) g_i(\bar{x})$ for some $g_i \in \mathbf{F}[x_1, \dots, x_k]$, where $|\mathbf{F}| = q$. This condition can be checked in linear time since we only need to divide g by $x_i^{q-1} - 1$ (i.e. substitute $x_i^{q-1} = 1$) for all $i \in \{1, \dots, k\}$ and the remaining expression has to be 0.

□

Theorem 10. *If $\mathbf{G} \simeq \mathbf{A} \rtimes \mathbf{B}$ where $\mathbf{A} \simeq \mathbf{Z_p}$ for some prime p, and* POL-EQ $\mathbf{B}$ *is in P then* POL-EQ $\mathbf{G}$ *is in P.*

Proof. The subgroup $\mathbf{B}$ acts on $\mathbf{A}$. Now, Aut $(\mathbf{A}) \simeq \mathbf{C}_{p-1}$, the cyclic group of order $p-1$ and consists of the maps $a \to a^l$ for every $a \in \mathbf{A}$ for some $1 \leq l \leq p-1$. Thus there is a homomorphism $\phi : \mathbf{B} \to \mathbf{C}_{p-1}$ such that $a^b = a^{\phi(b)}$ for every $a \in \mathbf{A}$. Now, using the collecting procedure it is enough to check whether or not $b_1 b_2 \dots b_k$, $a_j^{h_1} a_j^{h_2} \dots a_j^{h_l}$ and $c_1^{w_1} c_2^{w_2} \dots c_m^{w_m}$ are identities. The first condition can be checked in polynomial time by the assumption. For the second one we rewrite the expression $a_j^{h_1} a_j^{h_2} \dots a_j^{h_l} = a_j^{\phi(h_1)} a_j^{\phi(h_2)} \dots \ a_j^{\phi(h_l)} = a_j^{w_1+w_2+\dots+w_l}$. Here w_j denotes the image of h_j at ϕ. Substituting $\phi(b_j) = y_j$ we have w_j as a product of some of $y_1, \dots y_k$ over $\mathbf{Z_p}$, shortly a monomial, and $f = w_1 + w_2 + \dots + w_l$ is a k-variable polynomial over $\phi(\mathbf{B})$ where both the addition and the multiplication is understood in $\mathbf{Z_p}$. The expression $a_j^{w_1+w_2+\dots+w_l}$ is an identity if and only if f attains 0 every time when we substitute elements of $\phi(\mathbf{B})$ for the variables. And this can be checked in polynomial time by Lemma 9. Finally, $c_1^{w_1} c_2^{w_2} \dots c_m^{w_m}$ can be written in the form $c^{w'_1} c^{w'_2} \dots c^{w'_m}$, where c is the generator, of $\mathbf{A}$. Using the same idea, this is an identity if and only if $w'_1 + \dots + w'_m$ attains 0 every time when we substitute elements of $\phi(\mathbf{B})$ for the variables. And this can be checked in polynomial time by Lemma 9, again. □

Corollary 11. *If* $\mathbf{G} \simeq \mathbf{A} \rtimes \mathbf{B}$*, where* POL-EQ $\mathbf{B}$ *is in P, and* $\mathbf{A} \simeq \mathbf{Z_m}$ *where* m *is squarefree, then* POL-EQ $\mathbf{G}$ *is in P.*

Proof. Now, $\mathbf{A} \simeq \oplus_{p|m} \mathbf{Z_p}$ and all summands are $\mathbf{B}$ invariant. Every constant can be uniquely decomposed into a product of elements from $\mathbf{Z_p}$ for $p|m$. For a polynomial p let $t_{(p)}$ denote the polynomial when we replace each constant by its p part. Obviously, a polynomial is an identity over $\mathbf{G}$ if and only if $t_{(p)}$ is an identity over $\mathbf{Z_p} \rtimes \mathbf{B}$ for every prime p dividing m. This can be checked in polynomial time by Theorem 10.

□

Unfortunately the same idea does not work for a noncyclic normal subgroup, $\mathbf{A}$. The collecting procedure can be used in a few other cases, though.

Theorem 12. *Let* $\mathbf{G} \simeq \mathbf{A} \rtimes \mathbf{B}$ *such that the following hold:*

(a) $\mathbf{A}$ *is Abelian and the exponent of* $\mathbf{A}$ *is squarefree;*
(b) POL-EQ $\mathbf{B}$ *is in P;*
(c) *for ever prime* p *dividing the size of* $\mathbf{A}$ *and* $\mathbf{P} \in Syl_p(\mathbf{A})$ *the group* $\mathbf{B}/C_{\mathbf{B}}(\mathbf{P})$ *is Abelian and* $p \nmid |\mathbf{B}/C_{\mathbf{B}}(\mathbf{P})|$*, where* $C_{\mathbf{B}}(\mathbf{P})$ *denotes the centralizer of* $\mathbf{P}$ *in* $\mathbf{B}$*.*

Then POL-EQ $\mathbf{G}$ *is in P.*

Proof. After the collection procedure we see that it is enough to check identities over $\mathbf{B}$ and identities of the form (2)

$$a^{x_1^{k_{11}}x_2^{k_{12}}\ldots x_n^{k_{1n}}}a^{x_1^{k_{21}}x_2^{k_{22}}\ldots x_n^{k_{2n}}}\ldots a^{x_1^{k_{l1}}x_2^{k_{l2}}\ldots x_n^{k_{ln}}}, \tag{3}$$

and $c_1^{w_1}c_2^{w_2}\ldots c_m^{w_m}$ for the constants. The Sylow subgroups of $\mathbf{A}$ are $\mathbf{B}$ invariant, hence it is enough to check the identity for the Sylows of $\mathbf{A}$. Thus we may assume that $\mathbf{A}$ is an elementary Abelian p-group. Let $\mathbf{A} \simeq \mathbf{Z}_p^m$ and let $\varphi\colon \mathbf{B} \to \mathrm{Aut}\ \mathbf{Z}_p^m \simeq GL_m(\mathbf{Z}_p)$ be the action of $\mathbf{B}$ on $\mathbf{A}$, $\varphi(\mathbf{B}) = \mathbf{H}$. With these notations we need to check identity (2) for $\mathbf{G} \simeq \mathbf{Z}_p^m \rtimes \mathbf{H}$, where $\mathbf{H}$ is an Abelian matrix group acting faithfully on $\mathbf{Z}_p^m$ (note that $\mathbf{H} \simeq \mathbf{B}/C_{\mathbf{B}}(\mathbf{Z}_p^m)$). Let $\mathbf{S}$ denote the subring of the ring of m by m matrices generated by $\mathbf{H}$. Now (3) can be rewritten as:

$$a^{x_1^{k_{11}}x_2^{k_{12}}\ldots x_n^{k_{1n}}+x_1^{k_{21}}x_2^{k_{22}}\ldots x_n^{k_{2n}}+\cdots+x_1^{k_{l1}}x_2^{k_{l2}}\ldots x_n^{k_{ln}}} \tag{4}$$

and it is enough to check whether or not the exponent

$$x_1^{k_{11}}x_2^{k_{12}}\ldots x_n^{k_{1n}} + x_1^{k_{21}}x_2^{k_{22}}\ldots x_n^{k_{2n}} + \cdots + x_1^{k_{l1}}x_2^{k_{l2}}\ldots x_n^{k_{ln}} \tag{5}$$

is identically 0 in $\mathbf{S}$ when substituting the elements of $\mathbf{H}$. The ring $\mathbf{S}$ acts semisimply on $\mathbf{Z}_p^m$, because $p \nmid |\mathbf{H}|$. By Maschke's theorem $\mathbf{S}$ is a direct sum of matrix-rings. As $\mathbf{H}$ is commutative, $\mathbf{S}$ is commutative, as well, hence $\mathbf{S}$ is a direct sum of fields: $\mathbf{S} = \oplus_{i=1}^{s}\mathbf{F}_{q_i}$. Thus $\mathbf{H} \leq \mathbf{S}^* \simeq \oplus_{i=1}^{s}\mathbf{F}_{q_i}^*$. Let $\mathbf{H}_i$ denote the projection of $\mathbf{H}$ to its i-th coordinate. Expression (5) is identically 0 over $\mathbf{S}$ if and only if it is 0 at every substitution from $\mathbf{H}_i$ for every $i \leq s$. By Lemma 9 this can be checked in polynomial time, and so POL-EQ $\mathbf{G}$ is in P.

Finally, consider the identity $c_1^{w_1}c_2^{w_2}\ldots c_l^{w_m} = 1$. Here we can write every c_j as a linear combination of some fixed basis, $\{v_i\}$, of $\mathbf{A}$. Let $c_j = \prod v_i^{\lambda_{ji}}$. Thus, it is enough to check, whether $v_i^{\lambda_{1i}w_1}v_i^{\lambda_{2i}w_2}\ldots v_i^{\lambda_{li}w_l} = 1$ is an identity for all $1 \leq i \leq s$. The exponent has to be identically 0 over $\mathbf{H_i}$, and this can be checked in polynomial time by Lemma 9.

□

Corollary 13. *Let $\mathbf{G} \simeq \mathbf{A} \rtimes \mathbf{B}$, where $\mathbf{A}$ and $\mathbf{B}$ are Abelian groups, such that the exponent of A is squarefree and $(|\mathbf{A}|, |\mathbf{B}|) = 1$ then* POL-EQ $\mathbf{G}$ *is in P.*

Proof. The conditions of Theorem 12 trivially hold.

□

Now, we investigate the case when neither the size nor the exponent of the normal subgroup is squarefree. The modification of the Lemma 9 remains valid for cyclic groups.

Lemma 14. *Let $f(x_1, \dots, x_k) = w_1 + \dots + w_l$ be a sum of monomials in k variables over $\mathbf{Z}_{p^\alpha}$ $(p > 2)$ and let $\mathbf{H}$ be the $p-1$ element subgroup of $\mathbf{Z}^*_{p^\alpha}$. Then, for any $\mathbf{M} \leq \mathbf{H}$ it can be checked in polynomial time whether or not f vanishes on $\mathbf{M}$.*

Proof. Let a be a generator of $\mathbf{H}$ and let $\mathbf{M} = \langle a^t \rangle$. Putting $z_j = x_j^t$ we have $f(\bar{x})$ is identically 0 over $\mathbf{M}$ if and only if $f(\bar{z})$ is identically 0 over $\mathbf{H}$. We claim that a polynomial $f \in Z_{p^n}[x_1, \dots, x_k]$ admits this latter property if and only if $f = \sum(x_i^{p-1} - 1)g_i(\bar{x})$ for some $g_i \in Z_{p^n}[x_1, \dots, x_k]$. This condition can be checked in linear time. Since the exponent of $\mathbf{H}$ is $p-1$, if f is of the required form, it vanishes over $\mathbf{H}$. On the other hand, as the elements of $\mathbf{H}$ are pairwise incongruent mod p (not only mod p^α), the polynomial has to vanish over $\mathbf{Z}^*_p$, as well. By Lemma 9 this happens if and only if $f = \sum(x_i^{p-1} - 1)g_{i1}(\bar{x})$ mod p and so $f = \sum(x_i^{p-1} - 1)g_{i1}(\bar{x}) + pf_1 \mod p^\alpha$. Hence f_1 is vanishing $\mod p^{\alpha-1}$. By the previous arguments $f_1 = \sum(x_i^{p-1} - 1)g_{i2}(\bar{x}) \mod p$. Continuing in the same fashion we obtain that $f = \sum(x_i^{p-1} - 1)g_i(\bar{x})$. □

The following theorem is a generalization of Theorem 10:

Theorem 15. *Let $\mathbf{G} \simeq \mathbf{A} \rtimes \mathbf{B}$ such that the following hold:*

(a) $\mathbf{A}$ *is cyclic;*
(b) POL-EQ $\mathbf{B}$ *is in P;*
(c) *for ever prime p dividing the size of $\mathbf{A}$ and $\mathbf{P} \in Syl_p(\mathbf{A})$ we have $p \nmid |\mathbf{B}/C_{\mathbf{B}}(\mathbf{P})|$.*

Then POL-EQ $\mathbf{G}$ *is in P.*

Proof. Going along the lines of Theorem 12, we may assume that $\mathbf{A} \simeq \mathbf{Z}_{p^m}$. Moreover, after the collection procedure, it is enough to check identities over $\mathbf{B}$ and identities of the form $f = w_1 + w_2 + \dots + w_l = 0$ over $\mathbf{B}/C_{\mathbf{B}}(\mathbf{P})$ (Note that this works for the constant part, as well, since we can write every constant as a power of the generator of $\mathbf{A}$). As $\mathbf{B}/C_{\mathbf{B}}(\mathbf{P}) \leq \mathrm{Aut}(\mathbf{Z}_{p^\alpha})$, condition (c) implies that $\mathbf{B}/C_{\mathbf{B}}(\mathbf{P}) \leq \mathbf{H}$, where $\mathbf{H}$ denotes the $p-1$ element subgroup of $\mathrm{Aut}(\mathbf{Z}_{p^\alpha})$. If $p = 2$ then $\mathbf{H} = 1$, if $p > 2$, then identities can be checked in polynomial time over $\mathbf{B}$ and $\mathbf{H}$, by condition (b), and by Lemma 14, respectively.

□

3. Satisfiability

A modification of the collecting procedure and Lemma 9 will also help us to find out the complexity of the POL-SAT problem for some metacyclic groups, including S_3.

Theorem 16. *For any group* $\mathbf{G}$ *of order* pq *where* p *and* q *are primes* POL-SAT $\mathbf{G}$ *is in P.*

Proof. Consider the case when $\mathbf{G} \simeq \mathbf{A} \rtimes \mathbf{B}$ where $\mathbf{A} \simeq \mathbf{Z_p}$ and $\mathbf{B} \simeq \mathbf{Z}_q$. We may assume that $\mathbf{G}$ is not abelian, and so $p \neq q$.

Let $\{t, s\}$ be an instance of POL-SAT $\mathbf{G}$. We would like to know whether or not $t = s$ has a solution. Multiplying by s^{-1} and writing t for ts^{-1}, we have to solve $t = 1$. After the collecting procedure we obtain the following equation:

$$t(g_1 \dots g_k) = (b_1 b_2 \dots b_k) \cdot \left(a_1^{b_2 b_3 \dots b_k} a_2^{b_3 \dots b_k} \dots a_{k-1}^{b_k} a_k \right) = 1.$$

As p and q are coprime, both

$$b_1 b_2 \dots b_k = 1$$

and

$$a_1^{b_2 b_3 \dots b_k} a_2^{b_3 \dots b_k} \dots a_{k-1}^{b_k} a_k = 1.$$

must hold. Since $\mathbf{B}$ is cyclic, we can solve $b_1 \dots b_k = 1$ as a congruence mod q, and we can express one of the variables (say, b_1) using the other variables and constants: $b_1 = c \prod b_i^{k_i d}$, this is what a solution looks like mod q. Substituting this expression for b_1 in $t_1' t_2' \dots t_k' t' = 1$, we only need to check the complexity of the satisfiability of this latter equation under the constraint for b_1. By a similar argument as in the proof of Theorem 10 we arrive at the solubility of

$$a^{x_1^{k_{11}} x_2^{k_{12}} \dots x_n^{k_{1n}} + x_1^{k_{21}} x_2^{k_{22}} \dots x_n^{k_{2n}} + \dots + x_1^{k_{l1}} x_2^{k_{l2}} \dots x_n^{k_{ln}}} = 1,$$

where a is a generator of $\mathbf{A}$. Now, it is enough to check whether or not the exponent attains 0, that is whether or not

$$x_1^{k_{11}} x_2^{k_{12}} \dots x_n^{k_{1n}} + x_1^{k_{21}} x_2^{k_{22}} \dots x_n^{k_{2n}} + \dots + x_1^{k_{l1}} x_2^{k_{l2}} \dots x_n^{k_{ln}} = 0$$

has a solution over $\mathbf{Z}_p$. As p is a prime, this equation has no solution if and only if

$$(x_1^{k_{11}} x_2^{k_{12}} \dots x_n^{k_{1n}} + x_1^{k_{21}} x_2^{k_{22}} \dots x_n^{k_{2n}} + \dots + x_1^{k_{l1}} x_2^{k_{l2}} \dots x_n^{k_{ln}})^{p-1} = 1$$

is an identity. This can be checked in polynomial time by Lemma 9, hence POL-SAT $\mathbf{G}$ is in P. □

4. Problems

Klíma's example mentioned in the introduction suggests the following question:

Problem 1. Is there an algebra $\mathbf{A}$ such that POL-EQ $\mathbf{A}$ is hard and POL-SAT $\mathbf{A}$ is in P?

If there is an example, it will not be a group. Indeed, for a group $\mathbf{G}$ every instance $f_1 \equiv f_2$ of POL-EQ $\mathbf{G}$ can be rewritten in the form $f_1 f_2^{-1} \equiv 1$. If you can check the solubility of $p = a$ in polynomial time, then the only thing to do is to check the solubility of $f_1 f_2^{-1} = g$ for every $g \neq 1$. The two polynomials are equivalent if and only if none of these equations have a solution.

The smallest group not discussed in this paper is $\mathbf{S}_4$. This group can be considered as a semidirect product of $\mathbf{Z}_2^2$ and $\mathbf{S}_3$. Here, the exponent of the first group is squarefree, TERM-EQ $\mathbf{S}_3$ is in P, but the action of $\mathbf{S}_3$ is not Abelian. If we attack this problem using our technics, then after the collecting procedure, going along the lines of the proof of Theorem 12 or Theorem 15, we should discuss terms over $M_2(\mathbf{Z}_2)$ evaluated on the invertible elements.

Problem 2. Find the complexity of TERM-EQ $\mathbf{S}_4$ and POL-SAT $\mathbf{S}_4$.

References

[1] D. M. Barrington, P. McKenzie, C. Moore, P. Tesson, D. Thérien, *Equation satisfiability and program satisfiability for finite monoids*, Math. Found. Comp. Sci. (2000, Bratislava), 127-181.

[2] S. Burris, J. Lawrence, *The equivalence problem for finite rings*, Journal of Symbolic Computation **15** (1993), 67-71.

[3] M. R. Garey, D. S. Johnson, "*Computers and intractability*", W.H.Freeman & Co., San Francisco, 1979.

[4] M. Goldmann, A. Russell, *The complexity of solving equations over finite groups*, Proceedings of the Fourteenth Annual IEEE Conference on Computational Complexity, Atlanta, Georgia, May, 1999, 80-86

[5] H. Hunt, R. Stearns, *The complexity for equivalence for commutative rings*, Journal of Symbolic Computation **10** (1990), 411-436

[6] O. Klíma, *Complexity of unification and matching problems in the varieties of idempotent semigroups*, Int. J. of Algebra and Comp., to appear

[7] O. Klíma, *Complexity issues of checking identities in finite monoids*, manuscript

[8] B. Larose, L. Zádori, *Taylor terms, constraint satisfaction and the complexity of polynomial equations over finite algebras*, Int. J. of Alg. and Comp., submitted (2004)

[9] J. Lawrence, R. Willard, *The complexity of solving polynomial equations over finite rings*, manuscript (1997)

[10] S. Seif and Cs. Szabó, *The computational complexity of checking identites in simple semigroups and matrix semigroups over finite fields*, Semigroup Forum (2002)
[11] P. Tesson, D. Thérien, *Complete classifications for the communication complexity of regular languages*, STACS '03

E-mail address: ghorvath@cs.elte.hu
E-mail address: csaba@cs.elte.hu

Eötvös Loránd University, Department of Algebra and Number Theory, 1117 Budapest, Pázmány Péter sétány 1/c, Hungary